Title of the Research:

A study on the minimality of linear codes over rings

Makhan Maji
Registration No. : VB - 705 of 2011-12
Date of Admission: 29.07.2017

Supervisor: Dr. Kalyan Hansda
Department of Mathematics, Visva-Bharati University,
Santiniketan, West Bengal,
India.

SYNOPSIS

Keywords : codewords, linear codes, minimal linear codes, cyclic codes.

1 Introduction

In the seminal paper 'A mathematical theory of communication' [5] published on 1948, Claude Shannon showed that, given a noisy communication channel, there is a number, called the capacity of the channel, such that reliable communication can be achieved at any rate below the channel capacity, if proper encoding and decoding techniques are used. This marked the birth of coding theory, a field of study concerned with the transmission of data across noisy channel and the recovery of corrupted message.

Digital communication systems are designed to send messages from a message generating source to its target. The message generated by the source can be of many forms, such as speech, images, or plain text. For sources such as speech or images, a transducer is required in order to convert the source into digital signals, such as a microphone, or video camera. A transducer is also used at the final destination in order to convert the digital signal into whatever desired form, audio or visual. Once the message is generated, it is transmitted to the encoder.

The encoder, as the name implies, encodes the data. The altered data is then passed on through the channel. Channels include but are not limited to wireless and wired communications, as well as physical data storage devices. The received data then gets decoded, and this decoded message ends up at the target user. However, channels are prone to noise, whether it is human error or malfunctioning of equipment, the data may be altered in unpredictable manners. For the sake of simplicity, from here on we assume that all messages have been converted into digital signals, or data.

The motivation for error correcting codes stems from the requirements of transmitting data over real channels, which are frequently imperfect. One must encode the data that is supposed to be transmitted in a reliable way, such that any noise on a channel does not interfere with the actual data. One has to remember that the received message may not be the same as the original sent message. The required error correction is achieved by introducing redundancy to the transmitted data, this aids in the detection of errors and ensures the possibility of retrieving the original message. This may be done in a simple way of repetition, but this is not the only method of adding redundancy. Usually, complex algorithms are preferred to encode the data with the required redundancy. Shannon's noisy-channel coding theorem states that, under certain conditions, there are certain codes that make the probability of error arbitrarily small [5].

2 Brief History:

A q-ary code is a set of sequences of elements from the set $F_q = \{a_1, a_2, \ldots, a_q\}$ called the alphabet. A linear code of length n over the finite field $\mathbf{F}_q$ is simply a subspace of the vector space $\mathbf{F}_q^n$. Since linear codes are vector spaces, their algebraic structures often make them easier to describe and use than non-linear codes.

As a special case of linear codes, minimal linear codes have important applications in secret sharing and secure two-party computations. Constructing minimal linear codes with new and desirable parameters has been an interesting research topic in coding theory and cryptography. C. Ding, Z. Heng, Z. Zhou studied [2] minimal codes over finite fields.

The sets of minimal codewords in linear codes were considered for the first time in connection with a decoding algorithm by Tai-Yang Hwang in his paper entitled 'Decoding linear block codes for minimizing word error rate' [4]. Additional interest to them was sparked by a work of J.Massey, entitled 'Minimal Codewords and Secret Sharing' [3].

Let q be a prime power and $GF(q)$ denote the finite field with q elements. An $[n, k, d]$ code C over $GF(q)$ is a k-dimensional subspace of $GF(q)^n$ with minimum(Hamming) distance d. The support of a vector $\mathbf{v} = (v_1, v_2, \ldots, v_n) \in GF(q)^n$, denoted by Suppt($\mathbf{v}$), is defined by

$$\text{Suppt}(\mathbf{v}) = \{1 \leq i \leq n : v_i \neq 0\}$$

A vector $\mathbf{u} \in GF(q)^n$ covers another vector $\mathbf{v} \in GF(q)^n$ if Suppt($\mathbf{u}$) contains Suppt($\mathbf{v}$). We write $\mathbf{v} \preceq \mathbf{u}$ if $\mathbf{v}$ is covered by $\mathbf{u}$, and $\mathbf{v} \prec \mathbf{u}$ if Suppt($\mathbf{v}$) is a proper subset of ($\mathbf{u}$). A codeword $\mathbf{u}$ in a linear code C is said to be minimal if $\mathbf{u}$ covers only codeword $a\mathbf{u}$ for all $a \in GF(q)$, but no other codewords in C, i.e $\mathbf{u}$ does not cover any other linearly independent codewords of C. A linear code C is said to be minimal if every codeword in C is minimal.

A linear code of length n over a finite ring R is a submodule of the module R^n.

3 Scope of Work:

Minimality of linear codes have been studied over fields. We want to study minimality of special types of linear codes such as cyclic, quasi-cyclic codes etc. Further there is a vast scope to study the minimality of linear codes over rings.

4 Plan of Work:

Here we want to investigate the followings:

1. Minimal cyclic codes over fields.
2. Minimal quasi-cyclic codes over fields.
3. Minimal DNA-linear codes over fields.
4. Minimal linear codes over rings.

References

[1] C. Ding, Z. Heng and Z. Zhou, Minimal binary linear codes, *IEEE Trans. Inf. Theory*, DOI 10.1109/TIT.2018.2819196.

[2] C. Ding, Z. Heng and Z. Zhou, Minimal Linear Codes over Finite Fields, *arXiv:1803.09988v1[cs.TT]*.

[3] J. Massey, Minimal Codewords and Secret Sharing, *in Proc. Sixth Joint Swedish- Russian Workshop on Inf. Theory, Molle, Sweden*, 1993, 246249.

[4] Tai-Yang Hwang, Decoding linear block codes for minimizing word error rate, *IEEE Trans. on Information Theory*, IT-25 (1979), 6, 733737.

[5] C. E. Shannon, A math. theory of communication, *Bell System Technical J.*, **27(3)**, pp. 379-423, (1948).